UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FEDERAL TRADE COMMISSION, Plaintiff, v. FIRST DATA MERCHANT SERVICES LLC, a limited liability company, and CHI W. KO, a/k/a Vincent Ko, Defendants.	Case No. 1:20-cv-3867 **COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF**

Plaintiff Federal Trade Commission ("FTC"), for its complaint alleges:

1. The FTC brings this action under Sections 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b) and 57b, and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101–6108, to obtain permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and in violation of the FTC's Trade Regulation Rule entitled Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310.

SUMMARY

2. This is an action by the FTC for injunctive and equitable monetary relief against Defendants for opening merchant accounts and processing payments in connection with a diverse array of scams and frauds that caused tens of millions of dollars in harm to American consumers.

3. Defendants have opened merchant accounts and processed payments for at least four deceptive schemes that have been the subject of FTC or U.S. Department of Justice law enforcement actions ("the Schemes"). The Schemes included, but were not limited to, a debt relief scam that used deceptive telemarketing, business opportunity scams that used deceptive websites, and a criminal enterprise that used stolen credit card data to bill consumers without their consent. Defendants received fees for processing the Scheme's payments.

4. Defendant Chi "Vincent" Ko ("Ko"), through his company First Pay Solutions LLC ("FPS"), established merchant accounts for the Schemes and processed the payments they took from consumers. Specifically, Ko and FPS: (1) opened hundreds of merchant accounts for the Schemes in the names of phony entities and shell corporations; (2) provided Wells Fargo Bank with false or deceptive information to obtain merchant accounts; (3) ignored evidence that FPS's sales agents were engaged in fraud; and (4) failed to adequately underwrite, monitor or timely terminate merchants which it knew, consciously avoided knowing, or should have known were engaged in fraud.

5. Defendant First Data Merchant Services LLC ("First Data") is a global merchant services acquirer and payment processor that processes over $2 trillion dollars in annual payment volume in the United States through a variety of distribution channels and partnerships, including through independent sales organizations ("ISOs"), such as FPS. At all times relevant to the Complaint, First Data employed FPS and Ko to sell First Data's payment processing services.

6. For years, First Data processed payments for the Schemes, ignoring repeated warnings and direct evidence that merchants solicited by FPS and Ko were engaged in fraud. First Data also violated its own anti-fraud policies, and the rules of its acquiring bank and the credit card networks, by failing to adequately: (1) underwrite, screen, monitor, and/or oversee

FPS or its sales agents; (2) review FPS's merchant boarding, underwriting, and risk management processes; and (3) monitor or timely terminate the Schemes' merchant accounts.

7. Defendants knew, consciously avoided knowing, or should have known, that the merchants whose accounts they opened and transactions they processed were defrauding consumers. Starting in 2012, Ko and FPS approved hundreds of merchant applications for the Schemes that were facially false or deceptive, that depicted shell companies as bona fide businesses, or that described business activity that was prohibited by bank and card association rules. In early 2012, FPS staff told Ko that FPS was opening merchant accounts based on fraudulent applications. By April 2012, First Data had already questioned whether to continue a relationship with FPS based on its failure to adequately underwrite merchant accounts. For the next two and a half years, First Data and FPS continued to process payments for the Schemes while communicating about deceptive conduct and exorbitant chargeback rates associated with FPS's portfolio. At one point, FPS's merchants accrued over 300,000 chargebacks in less than one year, representing approximately 40% of First Data's excessive chargeback violations for its entire wholesale merchant business.

8. Throughout its relationship with FPS and Ko, First Data received repeated warnings and direct evidence that FPS's portfolio was permeated by fraud, yet continued to allow Ko and FPS to approve and open merchant accounts with minimal oversight until the end of 2014 when Wells Fargo terminated FPS's processing contract. In December 2014, Visa required First Data to pay $18.7 million restitution in connection with FPS's merchants and banned the company from boarding high-risk merchants until it could be audited by a forensic accounting firm. In April 2015, the audit found significant failures in First Data's risk management practices, including "no controls" over high-risk merchant boarding in its wholesale

merchant business, deficient merchant transaction monitoring, and failures in due diligence of its agents, like FPS and Ko.

9. In May 2015, First Data acquired FPS's merchant accounts, took over its office space, and hired most of its employees. In September 2015, First Data asked Wells Fargo to allow former FPS employees employed at First Data to resume soliciting high-risk merchants. Wells Fargo granted the request on the condition that the former FPS employees were not "associated with or related to Vincent Ko" and that First Data could confirm that "Vincent Ko has no influence."

10. In January 2017, First Data hired Ko as its vice-president of strategic partnerships. While at First Data, Ko has hired at least 15 sales agents to solicit prospective merchants.

11. Defendants' acts and practices have enabled a host of pernicious scams and frauds to permeate the credit card system. Without the processing services provided by the Defendants, the Schemes could not have obtained fraudulent merchant accounts to process their credit and debit card transactions with consumers.

12. By establishing merchant accounts in the names of shell corporations and processing transactions for the Schemes, Defendants caused substantial injury to consumers, resulting in tens of millions of dollars in illegal charges to hundreds of thousands of victims.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

14. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2), (c)(2), (d) and 15 U.S.C. § 53(b).

PLAINTIFF

15. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41–58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101–6108. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

16. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the TSR, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 57b, 6102(c), and 6105(b).

DEFENDANTS

17. Defendant First Data Merchant Services LLC ("First Data") is a Florida limited liability corporation with its principal place of business at 5565 Glenridge Connector NE, Atlanta, GA 30342. First Data provides payment processing services for businesses. At all times material to this Complaint, First Data has established merchant accounts for businesses and processed their credit and debit card transactions with consumers. First Data transacts or has transacted business in this District and throughout the United States.

18. Defendant Chi "Vincent" Ko is a former vice-president of First Data and the former owner and president of FPS. Until First Data acquired FPS's merchant accounts in May 2015, FPS was in the business of soliciting and referring merchants who wished to accept credit and debit card payments to processors and banks. At all times material to this Complaint, acting

alone or in concert with others, Ko has formulated, directed, controlled, had authority to control, or participated in the acts and practices of FPS, including the acts and practices set forth in this Complaint. Ko transacts or has transacted business in this District and throughout the United States.

COMMERCE

19. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

THE CREDIT CARD SYSTEM AND MERCHANT ACCOUNTS

20. Defendants are in the business of offering credit and debit card processing services to businesses and helping them to establish merchant accounts with a financial institution ("acquiring bank") that is a member of the credit card networks (i.e., Visa, Mastercard). Without access to a merchant account, businesses are not able to accept consumer credit or debit card payments.

21. Various entities act as intermediaries between merchants and acquiring banks. These entities include payment processors, independent sales organizations ("ISOs"), and sales agents that offer payment processing services to merchants.

22. To manage risk and fraud, the card networks impose operating rules and restrictions on registered members and third parties, including acquiring banks and ISOs. In turn, acquiring banks enter into contracts with payment processors and ISOs that require compliance with the bank's policies and procedures for conducting due diligence or underwriting on each prospective merchant and monitoring each merchant's transaction activity to manage risk.

23. Generally, businesses that apply for a merchant account must undergo an underwriting process intended to ensure that the applicant is a legitimate and creditworthy business and to weed out merchants engaged in illegal conduct. As such, payment processors typically scrutinize merchant account applications and may deny applications from businesses that present a high risk of fraud or are prohibited either by an acquiring bank or the card associations, such as debt consolidation services or get-rich-quick business opportunities.

24. At times material to this Complaint, First Data was a merchant services acquirer and payment processor that solicited merchants through its relationships with ISOs, including through FPS. In August 2010, FPS, First Data, and Wells Fargo entered a Merchant Program Processing Agreement (the "Processing Agreement"), under which FPS agreed to solicit prospective merchants on their behalf and to comply with certain obligations related to the underwriting, boarding, and monitoring of its merchants. In exchange for soliciting, boarding, and monitoring merchants, FPS and First Data earned commissions or "residuals" based on the volume of transactions generated by each merchant account. The greater the volume, the more FPS and First Data earned. Both FPS and First Data also earned a fee for processing each "chargeback," or transaction disputed by a consumer, incurred by their merchants. Chargebacks occur when customers contact their credit card issuing bank to dispute a charge appearing on their credit card account statement. One of the primary indicators of fraudulent or deceptive conduct is a high chargeback rate.

25. Under the Processing Agreement, FPS acted as a "Wholesale ISO," assuming responsibility for initial underwriting of prospective merchants and financial liability for chargebacks on the accounts in its merchant portfolio. Typically, if a Wholesale ISO is unable to pay chargeback liabilities for its merchants, the processor and acquiring bank must pay the

chargeback liabilities to the card associations so that consumers who successfully dispute transactions can be made whole. Thus, processors such as First Data try to reduce the likelihood of owing chargeback liabilities by requiring that their ISOs comply with card network rules and the acquiring bank's policies on merchant underwriting and monitoring.

26. The Processing Agreement required FPS to perform a due diligence review of prospective merchants, including a background investigation of the business and principals. Specifically, Wells Fargo's rules required for every merchant application: "Validate/verify the legitimacy of the business. Any material discrepancies should be documented, investigated and resolved. The source of the verification should be included in the merchant file or a detailed description of the verification source should be retained."

27. FPS was also prohibited under the Processing Agreement from soliciting merchants engaged in certain unacceptable business practices because they were presumptively illegal, violated card association rules, or created excessive risk exposure. The banned categories included, for example, businesses selling "debt consolidation services," "Get Rich Quick Opportunities," and "[a]ny merchant engaged in any form of deceptive marketing practices." Wells Fargo also prohibited FPS from soliciting merchants selling nutraceuticals through free-trial offers, unless specifically pre-approved by Wells Fargo.

28. FPS was also required to provide to First Data completed application materials, including underwriting support and documentation, for all of the merchants it referred. In turn, through its fraud detection software systems, First Data maintained access to merchant application information for merchants boarded by FPS.

29. The Processing Agreement required First Data to screen all merchants solicited by FPS against "negative file lists," which are databases of problem accounts that are used in the

underwriting process to identify potentially high-risk merchants. First Data also was required to check merchants against the card associations' lists of terminated merchants.

30. First Data and Wells Fargo ultimately retained the "sole right and authority to accept or reject any [merchant] Application" solicited by FPS.

31. In addition to the requirements of the Processing Agreement, Defendants were subject to industry rules and requirements designed to verify the identity of each prospective merchant and to screen out merchants potentially engaged in fraud, including card association rules, Wells Fargo and First Data's joint credit policy ("the joint credit policy"), and Wells Fargo's credit risk guidelines.

32. Once Defendants boarded a merchant, Wells Fargo's credit risk guidelines mandated that FPS "scrutinize [its] merchants" for evidence of deceptive marketing practices and, if found, "immediately compel the merchant to eliminate these practices or terminate the merchant." The guidelines also provided numerous examples of common warning signs of potential deceptive marketing practices, which included negative options, telemarketing, and high-pressure sales tactics, and listed industries where deceptive marketing practices were prevalent, such as debt consolidation, Internet-based work-from-home opportunities, and nutraceuticals.

33. Under the joint credit policy, First Data was responsible for monitoring the merchants solicited by FPS for indicators of fraudulent or deceptive activity. This monitoring process, in which a processor reviews the transaction activity of its merchants, is known within the payment processing industry as "shadow monitoring," the "shadow management process," or "back-end monitoring."

34. As part of its shadow monitoring process, First Data maintained access to data

regarding FPS merchants' processing activities, which enabled First Data to view and monitor credit card transactions, including individual transaction details, as well as monthly and year-to-date summaries of overall transaction and chargeback counts and volume for each merchant account.

35. Wells Fargo's credit risk guidelines specifically warned about "merchants' opening of multiple accounts, especially via multiple shell companies having the same or similar principals (in some cases, hired 'mules' with little or no business involvement may be submitted to obscure the true ownership)." Using multiple merchant accounts for the same business is a strong indication that a merchant applicant is "load balancing," a practice in which a business spreads its transactions among multiple merchant accounts to avoid triggering chargeback thresholds that would increase scrutiny from the credit card associations. The practice of processing credit card transactions through another company's merchant accounts is called "credit card laundering" or "factoring" in the credit card industry. It is strictly forbidden by the credit card associations and is illegal under the TSR.

36. As part of its oversight function under the joint credit policy, First Data was also required to review and approve FPS's fraud risk management processes, including systems, reports, and staffing, as well as FPS's merchant solicitation and underwriting procedures.

Defendants' Obligations to Underwrite and Monitor FPS's Sales Agents and to Refrain from Shifting Liability for Merchant Losses

37. From at least February 2012 to October 2014, FPS contracted with a variety of sales agents, or "sub-ISOs," across the country who specialized in soliciting "high risk" merchants. An acquiring bank or the credit card associations may designate as "high risk" merchants engaged in certain lines of business that may be more susceptible to fraud, resulting in

possible harm to a financial institution and consumers.

38. First Data was required to underwrite its ISOs like FPS, as well as sub-ISO sales agents that referred merchants to FPS. Under the joint credit policy, First Data and FPS were required to underwrite sub-ISOs, or "sales agents," through a "complete (full) review" of the agent, which was the most extensive due diligence review process outlined in the policy. A complete review included a background check and business history review of the sales agent, verification of its business references, on-site inspection of the sales agent's business location, evaluation of credit score, and verification that the sales agent was registered with Visa or Mastercard. Additional steps in the due diligence process listed in the joint credit policy were a BBB ratings review, litigation check, and Internet search analysis.

39. The joint credit policy also charged First Data with ensuring that FPS's sales agents did not own some or part of the underlying risk on a merchant account – that is, the liability for merchant losses if chargebacks from consumers exceeded a merchant's ability to pay. The policy explicitly forbade such an arrangement: "Under no circumstance should there be an indirect or hybrid sub-ISO…That is, the sub-ISO…may not own some or part of the underlying risk." In other words, FPS was forbidden from assigning liability for merchant losses to FPS's sales agents. Some acquiring banks prohibit this practice because an ISO which disclaims liability for chargeback losses may have less incentive to properly underwrite the accounts to ensure they are bona fide, creditworthy businesses that are not engaged in fraud.

40. During the relevant time period, FPS's high-risk sales agents included, but were not limited to: CardReady LLC ("CardReady"), Brandon Becker, James Berland, First Pay Systems LLC ("First Pay Systems") f/k/a Electronic Payment Services, Inc., KMA Merchant Services LLC ("KMA"), Jay Wigdore, Michael Abdelmesseh, and Richard Kuhlmann

(collectively, "the FPS Agents").

41. Like FPS and First Data, the FPS Agents made fees on the volume of merchants they boarded and processed.

The Schemes

42. As described in detail below, through the FPS Agents, Defendants processed payments for the following Schemes:

a. Thrive Learning: From at least February 2012 to February 2014, Defendants established merchant accounts and processed payments for Thrive Learning LLC and interrelated companies (collectively, "Thrive"). Despite clear indications in Thrive's merchant application packages that the business was a get-rich-quick opportunity prohibited by Visa with a history of telemarketing law violations, Defendants processed at least $3.5 million in Thrive's charges to consumers. In June 2017, the FTC sued the Thrive entities and entered into stipulated consent orders with them that contained a permanent injunction and monetary judgment. *See FTC v. Thrive Learning LLC et al.*, No. 2:17-cv-00529-DN (D. Utah 2017).

b. The Coaching Department: From at least February 2012 to February 2014, Defendants opened over 150 merchant accounts and processed payments for an enterprise that deceptively marketed work-at-home programs and business coaching programs (the "Coaching Department"). Defendants opened scores of merchant accounts for the Coaching Department and processed at least $20 million dollars through the accounts after FPS approved demonstrably false merchant applications that listed straw men as business owners and fictitious business locations. In February 2014, a federal court in Utah shut down the

scheme, and its operators later agreed to stipulated permanent injunctions and monetary judgments. *See FTC v. Apply Knowledge LLC et al*. (No. 2:14-cv-00088-DB) (D. Utah 2014).

c. E.M. Systems: From at least January 2013 to November 2014, Defendants established merchant accounts and processed payments for E.M. Systems & Services LLC ("E.M. Systems") through 26 shell companies. E.M. Systems operated a debt relief telemarketing scam that took over $20 million from consumers for approximately two years. Defendants opened merchant accounts for E.M. Systems's shell companies based on demonstrably false merchant applications that listed straw men as business owners and fictitious business locations. Defendants then processed E.M. Systems' payments through these shell accounts, as well as other shell accounts Defendants previously opened for the Coaching Department. In 2015, a federal court in Florida shut down the scheme, and E.M. Systems and its telemarketers subsequently agreed to a stipulated permanent injunction and entry of a partially suspended judgment of more than $12 million. *See FTC et al. v. E.M. Systems & Services LLC et al*., No. 8:15-cv-01417-SDM (M.D. Fla. 2015).

d. The Beckish Scheme: From at least February to November 2014, Defendants opened and serviced hundreds of merchant accounts for a criminal enterprise operated by James Beckish and other individuals (collectively, "Beckish") that used consumer's stolen credit card data to place at least $28 million in unauthorized charges on their bills without their knowledge or consent. First Data and FPS opened merchant accounts for the enterprises' demonstrably false

merchant applications, which listed phony websites that purported to sell dietary supplements (or "nutraceuticals") and web hosting services to consumers. Many of the applications approved by FPS listed the same maildrop as its business location or left the "business description" field blank. Equipped with merchant processing accounts, Beckish ran millions of dollars in unauthorized transactions on consumers' credit cards using their stolen card information. In June 2017, the U.S. Department of Justice indicted Beckish and associates on charges of wire fraud and aggravated identity theft. In October 2018, two of the defendants pled guilty to conspiracy to commit wire fraud in connection with a scheme to make unauthorized charges on credit cards through sham companies that purportedly offered nutraceutical products for sale over the internet. *See United States v. Beckish, et al*., No. 16-cr-00466 (S.D.N.Y 2017).

43. By granting and maintaining access to the credit card system with minimal or no oversight and ignoring direct evidence of illegal conduct, Defendants enabled perpetrators of the Schemes to initiate millions of dollars in illegal charges to consumers' credit and debit card accounts and evade detection by card associations, consumers, and law enforcement.

DEFENDANTS' DECEPTIVE AND UNFAIR BUSINESS PRACTICES

First Data and FPS Opened Hundreds of Straw Accounts for the Schemes Based on Facially False, Deceptive, or Blank Merchant Applications

44. First Data and FPS established hundreds of merchant accounts for the Schemes in the names of "straw men" or "mules" who had not given consent to their personal and financial information being used to apply for merchant accounts and often did not even know that merchant applications had been submitted in their names. These accounts were used, sometimes

interchangeably, to process consumer payments for the Schemes. First Data and FPS established these accounts after FPS approved merchant applications that were facially false or deceptive, contained obvious factual discrepancies or internal inconsistencies, omitted key information about the merchant applicant's business, or contained other "red flags," or obvious indicators of fraud.

45. In some instances, FPS approved merchant applications for the Schemes that had no business description, no marketing materials, no merchant category code, no employee information, and no other information identifying the goods or services the merchant offered to consumers.

46. In other instances, First Data and FPS opened accounts after FPS approved merchant applications that were demonstrably false, contained business descriptions that were prohibited by its Processing Agreement with Wells Fargo, violated bank or card brand rules, or demonstrated histories of telemarketing law violations.

First Data and FPS Opened 100 Straw Accounts for the Beckish Scheme Based on Blank or Copycat Applications

47. From January to October 2014, First Data and FPS opened at least 100 merchant accounts in the names of purported dietary supplement and web hosting companies that never legitimately sold any products or services. Once opened, these sham accounts were used by the Beckish Scheme to bill consumers at least $28 million without their consent, using their stolen credit card data. First Data and FPS opened these accounts after FPS approved merchant applications that were substantially blank, duplicate, or contained other obvious indicators of fraud.

48. For example, from March to July 2014, First Data and FPS opened at least 20

accounts after FPS approved merchant applications that were substantially blank and that failed to provide any required information about the applicant's business, employees, advertising method, marketing materials, trade references, or refund policies. All the applications listed the same mail drop in Grandville, Michigan as the applicants' business location and were submitted by the same sales agent. In numerous instances, the only business-identifying information on the merchant application was a non-functional or fictitious website address.

49. During the same time period, from February to September 2014, FPS approved 40 pairs of identical merchant applications. Each pair had the same purported principal and merchant name and was opened the same day. Using multiple merchant accounts for the same business – let alone submitting identical merchant applications – is a strong indication that the merchant applicant is "load balancing," a practice in which a business spreads its transactions among multiple merchant accounts to avoid triggering chargeback thresholds that would increase scrutiny from the credit card associations.

50. These pairs of identical merchant applications also used suspicious billing descriptors that hid or omitted the merchant's name. For example, FPS approved merchant applications for purported nutraceutical and web hosting companies with billing descriptors that contained no text except for the phone number to an offshore telemarketing call center – *e.g.* 888-441-2916.COM. Merchant applicants which fail to use their business name in billing descriptors are red flags for payment processors, and payment processors who board such applicants violate credit card association policies intending to ensure that consumers can identify the business charging their debit or credit cards.

First Data and FPS Opened 26 Straw Accounts for the E.M. Systems Scheme Based on Facially False Applications and Despite Indicators of Fraud

51. From November 2012 to October 2014, First Data and FPS opened at least 26 merchant processing accounts for shell companies that were used by the E.M. Systems Scheme to charge consumers in a deceptive debt relief scam. First Data and FPS opened these accounts even though the merchant applications submitted contained facially false statements, direct evidence, or other red flags that the applicants were not bona fide businesses or were engaged in fraud.

52. In May 2013, for example, First Data and FPS opened a merchant account for a purported personal budgeting web portal called "Budgeting Insights." Despite the objection of a FPS staff member who noted that the web portal was "not operable" and "identical to the website for Insightful Budgeting," another shell entity used by the E.M. Systems Scheme, the account was opened.

53. In July 2013, First Data and FPS opened a merchant account for Del Rey Products LLC, a purported personal finance coaching business. Even after FPS staff acknowledged that the application falsely described the merchant's business and that it was in fact "offering credit repair/restoration services, which is an unqualified business type," the account was opened the same day.

54. First Data and FPS also opened two merchant accounts for Level Services LLC after FPS approved contradictory merchant applications. In the first application, the company purportedly had a first-floor storefront with 20 employees, while the second application described a second-floor storefront with five employees. Neither application listed a business address that matched the location description. In regard to the second account, FPS staff noted

that "some of the information on the MPA [merchant processing agreement] does not match the merchant's driver's license." Despite staff's email, the account was opened later the same day.

55. In October 2013, First Data and FPS opened a merchant account in the name of Sensible Budgeting. According to the merchant application, Sensible Budgeting operated a storefront on 2-4 floors with numerous employees, yet the listed business address was a residential apartment unit.

56. In February 2014, First Data and FPS opened an account in the name of Intuitive Budgeting, a business that purported to have 2-4 floors of office space, yet the listed business address was a single floor residential apartment unit.

First Data and FPS Opened 150 Straw Accounts for the Coaching Department Scheme Based on Facially False or Deceptive, Blank, or Internally Inconsistent Applications

57. From at least March 2012 to February 2014, First Data and FPS opened over 150 merchant processing accounts for shell companies that were used by the Coaching Department Scheme to charge consumers in a deceptive business coaching operation, based on merchant applications that contained false statements, internal inconsistencies, or other hallmarks of fraud.

58. In March 2012, for example, First Data and FPS opened an account for Vi-Education LLC, a purported "online education and training" website, even though the website listed on the merchant application was non-functional. The application also included an outbound telemarketing sales script, yet FPS approved the account without registering the merchant as an outbound telemarketer, in violation of Visa and Mastercard policies.

59. Also in March 2012, FPS approved an account for Gila Marketing LLC, another purported online training website, based on a partially blank merchant application that omitted information about the applicant's business site, number of employees, or refund policies.

Moreover, a website screenshot attached to the application did not match the web address listed in the body of the application.

60. In May 2012, FPS received a merchant application for Meacham Moose LLC, a purported online education company doing business as Partner Education. According to the application, the company operated in a commercial office space with five employees, yet the listed business address was a residential home. First Data wrote to FPS with concerns that "the business name does not match the [merchant account name]." Despite these reservations, First Data and FPS opened the account.

61. In August 2012, First Data and FPS established a merchant account for Nesch.edu, a purported financial coaching business, after FPS approved an apparently doctored application and despite the applicant's prior termination for excessive chargebacks for the same business activity. In the application, the "business name" field was whited-out and handwritten, while the rest of the application was typed. The business location was described as an office with 2-4 floors, yet the address provided was a single-floor residential apartment unit. After receiving the application, FPS emailed internally, noting that the application had a prior account under a different business name that was closed two weeks earlier for excessive chargebacks and refunds: "the new application's business model is the same as the previous account." Yet days later, FPS approved the new account and First Data began processing its charges. In fact, both accounts were used by the Coaching Department to bilk consumers as part of a deceptive telemarketing scam.

62. In April 2013, First Data and FPS opened four merchant accounts based on applications that listed identical mail drops as their business locations, contained identical marketing materials, and included identical articles of incorporation.

First Data and FPS Opened Accounts for Thrive Learning Despite Evidence That It Was a Get Rich Quick Scheme with a Record of Telemarketing Law Violations

63. First Data and FPS opened at least four merchant accounts for the Thrive Learning Scheme based on applications that described business practices that were illegal, suspicious, or prohibited by Wells Fargo and the credit card associations.

64. Under the Processing Agreement, FPS was prohibited from boarding specific "illegal or likely to be deemed illegal" businesses, which included "get-rich-quick opportunities."

65. In February 2012, FPS approved a merchant application for Thrive LLC that stated that the company was a "100% telephone order merchant" and included a telemarketing sales script that promised consumers could "make some quick cash on Ebay." The application package also contained a "Government Action" notice from Thrive's Better Business Bureau profile describing a 2009 law enforcement action against Thrive by the State of Utah regarding its practices of telemarketing business coaching services with "guarantees or promises of success or money back." By May 2012, FPS had approved at least four additional merchant accounts for Thrive with the same principal, merchant name, address, DBA or website. Three of the applications identified Thrive LLC as the applicant's parent corporation and vendor and attached bank statements or tax returns for Thrive LLC.

All Four Schemes Came From FPS Sales Agents Who Had Publicly-Available Criminal or Problematic Backgrounds

66. Under First Data and Wells Fargo's joint credit policy, First Data and FPS were required to underwrite sub-ISOs, or "sales agents," through a "complete (full) review" of the agent, which was the most extensive due diligence review process outlined in the policy. A complete review included a background check and business history review of the sales agent,

verification of its business references, on-site inspection of the sales agent's business location, evaluation of credit score, and verification that the sales agent was registered with Visa or Mastercard. Additional steps in the due diligence process listed in the joint credit policy were a BBB ratings review, litigation check, and Internet search analysis.

67. First Data and FPS failed to adequately underwrite or conduct due diligence on the FPS Agents who submitted merchant applications for the Schemes. In fact, many of these agents had criminal backgrounds or problematic business profiles at the time they contracted with FPS. This information was obtainable through basic due diligence, such as public records searches or background check services.

68. FPS Agents Jay Wigdore, Richard Kuhlmann, and KMA, a company operated by Wigdore and Michael Abdelmesseh, submitted merchant applications for the Beckish Scheme. At the time they began submitting applications to FPS in January 2014:

a. Wigdore had federal criminal convictions in 1995, 2000, and 2003 for mail fraud, bank fraud, and conspiracy to commit fraud. Wigdore's illegal conduct was also highlighted in the FBI's publicly available 2004 "Financial Institution Fraud and Failure Report." At the time Wigdore contracted with FPS, his convictions were public and the FBI report was available on the Internet.

b. KMA maintained an "F" ranking with the Better Business Bureau ("BBB") for at least two years prior to contracting with FPS. KMA's ranking was publicly available on the BBB's website at the time it began referring merchants to FPS and First Data.

c. Kuhlmann was subject to numerous publicly available civil judgments and tax liens during the five-year period before becoming an FPS sales agent.

69. From March 2012 to July 2014, FPS Agent CardReady submitted merchant applications for the E.M. Systems, Coaching Department, and Thrive Learning Schemes. At the time it contracted with FPS, in February 2012, CardReady and its CEO faced an unpaid civil judgment of approximately $700,000 for breach of contract that was public record. CardReady was also named as a defendant in a fraudulent conveyance action that was public record during the time period it referred merchants to FPS and First Data.

70. Provisions in FPS's contracts with its agents also violated Wells Fargo and First Data's joint credit policy, which prohibited sales agents from personally guaranteeing or otherwise accepting the risk of loss on merchant accounts. According to the contracts, the FPS Agents retained some or all of "the risk," or liability for merchant losses that resulted from consumer chargebacks. An ISO's assigning to a sales agent liability for chargeback losses on high-risk merchant accounts was not only prohibited by Wells Fargo and First Data, but is a strong indicator that the ISO is aware that the merchant applicants referred by the sales agent are generating, or likely to generate, excessive rates of chargebacks. First Data failed to timely or adequately review FPS's contracts with the Agents, which would have revealed a risk-sharing arrangement that was in direct conflict with its own rules.

71. First Data ignored publicly available information and failed to conduct adequate due diligence or underwriting measures to learn about the FPS Agents' criminal pasts, problematic histories, and improper contracts, all of which violated Wells Fargo's and First Data's policies. As a result, the FPS Agents were allowed to submit merchant applications for the Schemes into the credit card system, costing consumers millions of dollars in illegal charges.

FPS's President Knowingly Approved or Directed His Staff to Approve, False or Deceptive Merchant Applications for the Schemes

Ko Told Staff to Unconditionally Approve Applications from CardReady

72. In early 2012, FPS underwriting staff told Ko in numerous meetings that certain sales agents appeared to be submitting false or deceptive merchant applications to FPS. During one or more of these meetings, FPS staff described to Ko their prior business dealings with one of the FPS's sales agents, CardReady, including instances in which CardReady had submitted false or deceptive merchant applications to other ISOs. FPS staff and Ko also discussed CardReady's reputation within the payment processing industry as being associated with consumer fraud. Rather than addressing the concerns raised in the meetings, Ko instructed staff to unconditionally approve merchant applications from CardReady, which included accounts for the Coaching Department, E.M. Systems, and Thrive Schemes.

73. On numerous other occasions in 2012, an FPS manager told Ko that the underwriting department had detected groups of prospective merchant applications from CardReady that appeared to be shell companies or whose applications contained false information. In numerous instances, Ko ignored the manager's concerns and instructed her to approve and open accounts for the identified fraudulent applications.

74. Later still in 2012, additional FPS staff members told Ko that they refused to sign off on merchant applications that FPS had received from CardReady because they contained false or deceptive information. At or around the same time, Ko bypassed FPS's underwriting department and directed CardReady to submit merchant applications directly to Ko or to FPS's new accounts department. After such submissions, Ko or staff in the new accounts department would rubber stamp the applications. Ko told CardReady's CEO to send FPS more high-risk

business throughout 2013, which included accounts for the Coaching Department and E.M. Systems Schemes.

75. In August 2013, Ko received an email from CardReady advising him that the billing descriptor for an E.M. Systems merchant account needed to be changed so it could be used to process transactions for a separate business that sold dietary supplements. FPS switched the billing descriptor and processed transactions through the account under the new billing descriptor. A merchant's use of multiple billing descriptors to mask the merchant's true identity or activity is a common tactic used by fraudsters to evade scrutiny by the credit card associations and law enforcement. At the time FPS processed for the Schemes, Wells Fargo's credit risk guidelines specifically warned that multiple billing descriptors were a "**tactic[] to evade chargeback monitoring programs.**" (emphasis in original).

Ko and FPS Ignored Evidence that First Pay Systems Was Submitting Fraudulent Merchants For the Beckish Scheme

76. In December 2013, FPS entered negotiations with another sales agent, First Pay Systems LLC ("First Pay Systems") f/k/a Electronic Payments Services Inc., to board more high-risk merchants. During the negotiations, FPS's director of risk and underwriting emailed Ko that First Pay Systems' principal Richard Kuhlmann had "overloaded the New Application email box" before a signed sales agreement was in place. The email continued: "We mUST (sic) have an agreement where he is taking liability." In January 2014, FPS executed an agreement with First Pay Systems to split 50/50 all fee revenue and liability for merchant losses in direct violation of Wells Fargo and First Data's joint credit policy.

77. In February 2014, Ko received a background report showing that First Pay Systems' principal Jay Wigdore had federal criminal convictions in 1995, 2000, and 2003 for

mail fraud, bank fraud, and conspiracy to commit fraud, including convictions related to falsifying credit applications and credit bureau reports. Yet after receiving the report, Ko and FPS continued to accept merchant applications from Wigdore and First Pay Systems, including accounts for the Beckish Scheme.

78. In June 2014, Ko received a letter from a merchant claiming that proceeds from his business had been diverted into a merchant account fraudulently boarded by First Pay Systems, Wigdore, and Richard Kuhlmann:

> Your Arizona affiliate [First Pay Systems] is a rogue agency and apparently a criminal enterprise…
>
> The Agent submits false applications containing cut and paste bank checks designed to purportedly represent the merchant acct. when in reality the funds are diverted back to themselves…
>
> They submit phony web sites that do not represent the true nature of the merchant's business, knowing the correct website would not qualify…There are by in large known, illegally operated company's (sic) that cannot obtain a merchant acct. by legitimate means…
>
> They are the subjects of state and federal investigations (see subpoena).
>
> In the Nutraceutical space and others, they illegally compile large amount of 'nominee' applicants designed to circumvent chargebacks, returns and illegally 'load balance' a merchant's processing….
>
> They have committed theft, forgery, ID theft, bank fraud, and money laundering offenses. My money has been diverted to bank accounts to which I'm not even a signer.
>
> Jay Wigdore…and Richard Kulhman (sic) have criminal records. Kulhman has been 'black balled' everywhere in this industry with the exception of [FPS].

79. After Ko received and forwarded the letter to FPS's director of risk and underwriting, FPS continued to open merchant accounts submitted by Wigdore, Kuhlmann, and First Pay Systems – including approximately 50 new accounts for the Beckish Scheme – until it

was forced to stop in November 2014, at or around the time that Wells Fargo terminated its Processing Agreement with FPS and First Data.

80. By accepting, approving, and submitting to Wells Fargo merchant applications from the FPS Agents that he knew, consciously avoided knowing, or should have known contained false or deceptive information, Ko allowed the Schemes to process payments from consumers through hundreds of shell companies. This practice prolonged the Schemes' harm to consumers by obscuring their true perpetrators, enabling the Schemes to evade law enforcement and industry controls.

First Data and FPS Continued to Process for the Schemes Despite Red Flags and Direct Evidence that Their Merchants Were Engaged in Fraud

81. After the Schemes' merchant accounts were opened, First Data and FPS processed payments through the accounts even in the face of direct evidence or strong indicators that the underlying merchants were deceiving consumers, engaging in illegal activity, conducting business prohibited by the credit card associations, or accruing exorbitant chargeback rates. For example:

First Data and FPS Processed Millions for the Beckish Scheme Despite Evidence that Its Purported Nutraceutical and Webhosting Merchants Were Phony

82. In March 2014, First Data and FPS began processing for a group of purported dietary supplement, or "nutraceutical," merchants who were boarded the same day and had almost identical phone numbers and billing descriptors. A few weeks later, First Data flagged the accounts as experiencing a "high amount of chargebacks" and asked FPS, "why [do] they have multiple accounts?" In May 2014, Wells Fargo identified the group of purported nutraceutical merchants as fraudulent and interrelated, and Visa placed the merchants in its chargeback monitoring program. By this time, First Data and FPS had processed over $3 million

through the accounts.

83. In response, Wells Fargo banned FPS from boarding any nutraceutical accounts and noted in a presentation to First Data about the incident: "**FD's actions** – none; in fact, even when prompted to look for red-flags, no connection was made." (Emphasis in original).

84. Yet after the incident, First Data continued to process transactions through FPS's purported nutraceutical accounts throughout 2014. A June 2014 risk monitoring report circulated internally at First Data identified numerous clusters of FPS merchant accounts that were using apparently nutraceutical-related websites and billing descriptors (*e.g.*, PerfectSlimmingX.com / PRFCTSLMMNGCX), were opened on the same day under the same or similar merchant names, and had accrued excessive chargebacks. For example:

a. The report identified eight FPS nutraceutical accounts with related billing descriptors under the name JRC Capital or JRS Capital that had processed approximately $340,000 with an average combined chargeback and refund rate of 8%. After receiving the report, First Data continued to process an additional $425,000 through the accounts.

b. The report identified four FPS nutraceutical accounts opened the same day under the name Finn Holdings that had an average 6% combined chargeback and refund rate. First Data continued to process an additional $250,000 through the Finn Holding accounts after receiving the chargeback and refund information.

c. The report identified two FPS nutraceutical accounts boarded on the same day in April 2014 under the name HN Marketing LLC. Within weeks of opening, the account had processed approximately $30,000 with an average combined chargeback and refund rate of 5.75%. After receiving this information, First Data

continued to process an additional $330,000 through the accounts through September 2014.

85. First Data also received early indications that numerous purported webhosting accounts were experiencing high chargebacks and refunds in the first weeks of opening, yet continued to process millions of dollars through the accounts. For example, First Data received information in June 2014 indicating that a merchant whose DBA was Glorious-Hosting.com had a combined chargeback refund rate of 6% within its first month of processing. Despite this red flag, First Data continued to process an additional $380,000 through the account until it was identified by Wells Fargo as one of the "First Pay bad accounts" in September 2014.

86. In July 2014, First Data emailed internally that FPS had boarded approximately 25 more merchants that were "a string of new 'webhosting' accounts being opened by same owner located in Panama. All accounts have same NOB [nature of business] and webpage design. All accounts are new and have all fraud related chargebacks." In August 2014, a Wells Fargo risk manager emailed a First Data's risk director about the accounts, noting that [w]hen we called one of the toll free numbers they advised they were a call center that provides customer service for over 3,000 merchants. They appeared to be offshore …would appear to be in Panama." Around the same time, a First Data risk manager emailed FPS's director of underwriting and First Data's vice-president of risk management:

> We have an issue brewing with a large amount, dozens of recently boarded accounts. Recently we have seen a large amount of Webhosting accounts that have been boarded by [FPS]. All are the same business models with similar websites. All websites were opened by the same registrant and acquired offshore. The registrant is opening these Webhosting Accounts from a location based in Panama. This is easily confirmed by searching godaddy.com…They all are receiving fraud related chargeback's (sic).

87. Despite these overt indicators of fraud, First Data and FPS continued to process

over $17 million in unauthorized charges through these webhosting accounts after they were flagged as deceptive.

First Data and FPS Processed for the Coaching Department Scheme Despite Evidence that its Merchants were Interrelated and Deceptive

88. In April 2012, First Data emailed FPS about 10 business coaching accounts that had accrued combined refund and chargeback ratios of 27–36%: "[T]he [web]sites have identical terms and conditions and refund language. It goes right down to the same misspellings… All were boarded in February, have the same business model, are located in the same areas…and use identical terms and conditions. In addition all accounts have chargeback and refund issues." Disregarding these red flags, First Data and FPS continued to process at least $3.2 million in illegal charges through these accounts after they were identified.

89. In June 2012, a First Data risk director told FPS about a similar suspicious business coaching account boarded by FPS: "I believe the account is unqualified due to deceptive marketing practice…[I]ts website vi-education.com has had its registration expire with GoDaddy.com so it is suspended and available for sale." Despite these indicators of fraud, First Data and FPS continued to process consumer payments for the account through September 2012, processing an additional $1.3 million in consumer charges after the entity was flagged as deceptive.

90. In June 2012, a First Data risk manager flagged another business coaching account with the same characteristics that had an 11% chargeback ratio for May 2012, expressing concerns about likely fraudulent activity. Despite the manager's concerns, First Data continued to process for the account until October 2012, processing an additional $500,000 in illegal charges.

91. In September 2012, First Data and FPS began processing transactions for Nesch.edu ("Nesch"), another purported financial coaching business, even while FPS acknowledged internally that a prior merchant account for Nesch was closed in August 2012 "due to excessive chargebacks and high refunds" and the new application's business was "the same model as the previous account." Defendants continued to process approximately $330,000 through the account, from September 2012 to February 2013.

First Data and FPS Processed for the E.M. Systems Scheme
Despite Evidence of Deceptive Telemarketing

92. In April 2013, First Data emailed FPS about a newly boarded merchant, Martan LLC ("Martan"), that was experiencing excessive chargebacks and a "large amount of cardholder disputes" for "non-receipt of services" and "fraud related reasons." Despite observing these indicators of fraudulent activity, First Data and FPS continued to process $470,000 through the account until October 2013. In November 2013, First Data flagged another Martan account as having a 5% chargeback rate for non-receipt for services, yet Defendants continued to process an additional $1.4 million in consumer charges through the second account until February 2014. In all, First Data and FPS processed over $1.8 million in fraudulent transactions for Martan after First Data first identified the company as deceptive in April 2013.

93. In October 2013, First Data and FPS exchanged emails about excessive chargebacks on an account for "Today's Financial Living." In November 2013, First Data told FPS that Today's Financial Living had a 6% year-to-date chargeback ratio for "non-receipt of services." Disregarding these indicators of fraud, Defendants continued to process an additional $1 million for Today's Financial Living until February 2014.

94. In April 2014, First Data and FPS discussed chargeback notifications stating that a purported household budgeting service called Conserved Budgeting boarded just weeks earlier was telemarketing debt reduction services and that consumers were not receiving the services as promised. Again, in June 2014, First Data told FPS that Conserved Budgeting's purported website was non-functional, and that Mastercard had reported fraud sales in March and April 2014 for "non-receipt of services." Despite this evidence of consumer deception, Defendants did not stop processing transactions through the account until mid-September 2014, even as the merchant accrued an overall chargeback ratio of 6.35%, reaching 17.2% in July 2014. Defendants processed over $1.1 million in consumer payments through the account after receiving notice of Conserved Budgeting's improper practices in April 2014.

First Data and FPS Processed for the Thrive Accounts Despite Overt Indicators of Fraud

95. In July 2012, a First Data credit officer emailed an FPS risk manager: "I also did a check on [Thrive LLC] and found numerous complaints against them along with government action. I am having our credit policy review this as well, to assure it fits [First Data] credit policy." The email included numerous links to online consumer complaint boards and blogs that identified Thrive and affiliates as the perpetrators of numerous business coaching telemarketing scams. One of the blogs listed in the email, http://thrivescammedme.blogspot.com, displayed an entry titled "How Obtain a Refund If You've been Scammed by Thrive or Their Affiliates" and included model refund request letters for Thrive victims and contact information for the FTC, FBI, and Better Business Bureau ("BBB"). Another post on the blog was titled "Beware of Thrive Learning LLC and Affiliates" and included a consumer's first-person account of their experience with a Thrive telemarketer. The account described "high pressure sales calls" that promised that the consumer would "make between $100,000 and $250,000 per year with [their]

website, or online store, utilizing drop shipping services." According to the account, the consumer made no money and was unable to obtain a refund from the company. First Data's email also identified and described a consent decree entered into by Thrive LLC and the Utah Division of Consumer Protection involving telemarketing claims.

96. Despite these indicators of deceptive practices, Defendants continued to process consumer payments through Thrive LLC's merchant account and at least three other accounts whose application packages identified Thrive LLC as their parent corporation and vendor. In February 2013, Thrive LLC's merchant account generated a combined chargeback and refund rate of at approximately 7.5%. The rate remained constant through April and May 2013, grew to 9% in July 2013, and reached 62% in August 2013. Defendants continued to process consumer payments through the Thrive LLC account until October 2013.

First Data's Internal Records Demonstrate Awareness and Disregard of FPS's Systemic Boarding of Fraudulent Merchants

97. First Data's internal records indicate that First Data was aware of, and chose to ignore, repeated warnings about FPS's systemic boarding of fraudulent merchants.

First Data Questioned the Adequacy of FPS's Controls in 2012

98. In April 2012, First Data internally identified a group of merchants boarded by FPS who were marketing business coaching services and had accrued excessive chargebacks. After raising concerns that the accounts were interrelated and submitted by the same sales agent, a First Data senior risk manager escalated the issue to her supervisor to "see if we are comfortable working with this ISO relationship." In May 2012, the supervisor emailed FPS about its problematic merchant activity and noted, "I have reviewed the accounts with Senior Management." In fact, these accounts were shell entities for the Coaching Department Scheme.

99. In August 2012, based on the boarding of these accounts, Wells Fargo and First Data classified FPS as an "Excessive Risk ISO." The Excessive Risk ISO Program is a remedial program in which an ISO that violates certain bank and card brand policies is subjected to heightened monitoring. The heightened monitoring included monthly meetings between Wells Fargo and First Data risk management staff who produce "scorecards" that track the ISO's processing statistics and policy compliance. FPS was placed into the program based on its boarding of merchant accounts with excessive chargebacks.

100. In September 2012, a First Data risk manager wrote in an internal email about FPS, "I would scrutinize anything that comes from this ISO, based on [its] record."

101. In October 2012, a First Data risk manager summarized her concerns about FPS in an email to First Data's regional business director: "[A] review of the ISO portfolio and the dramatic increase in overall chargeback activities insinuated that the ISO are [sic] not addressing and terminating problematic accounts in a timely manner." The risk manager noted that FPS had submitted a remediation plan to address its "risk monitoring failures," but that the plan "did not address the root cause for signing unqualified accounts and preventive steps to ensure that this does not happen again."

102. In December 2012, Wells Fargo and First Data identified approximately 65 merchants for the Coaching Department Scheme with "identical business models" engaged in "deceptive marketing and/or billing practices due to non-disclosure of auto rebilling practices to cardholders" with 2012 year-to-date chargeback ratios ranging from approximately 14 to 33%.

103. In January 2013, as part of the Excessive Risk ISO review process, Wells Fargo and First Data graded FPS as a "Fail" and cited 70 card brand policy violations in 2012. In the remediation plan for FPS, First Data and Wells Fargo designated "Self-Cure" as the remediation

needed, while the "Enhanced Oversight" field was marked "No."

Law Enforcement and Industry Players Warned First Data about Fraudulent Accounts at FPS Yet First Data Continued to Process for FPS Merchants

104. In October 2012, First Data was contacted by the Utah Attorney General's Office in connection with FPS merchants for the Coaching Department Scheme that had scammed consumers.

105. In February 2013, First Data was contacted by Canadian law enforcement authorities about FPS merchants for the E.M. Systems Scheme who were processing charges for a scam in which telemarketers promised to lower the consumer's credit card interest rates yet provided no services, as well as other FPS merchants who were billing consumers for nutraceutical products that consumers never purchased.

106. In April 2013, Wells Fargo arranged a meeting with First Data and FPS staff about growing concerns with the FPS merchant portfolio. In discussion points emailed to First Data, Wells Fargo identified the issues and concerns to be discussed at the meeting as FPS's "boarding of unqualified accounts" and FPS's "merchant accounts engaged in deceptive practices."

107. In an attachment to the email, Wells Fargo identified names of over fifty FPS merchants which it said were either recently terminated, cited for engaging in outbound telemarketing, or were unqualified businesses under Visa rules, including accounts for the Coaching Department and E.M. Systems Schemes. Wells Fargo also warned First Data in an April 2013 email that FPS was "now dabbling into the risky nutraceutical; pseudo-pharmaceutical space," which was a banned category of business under Wells Fargo's credit policies when marketed with free-trial offers.

108. Wells Fargo, FPS, and First Data staff met in April 2013 at the Electronic Transactions Association Conference in New Orleans, Louisiana, to discuss FPS's problematic underwriting practices and merchants who were engaged in deceptive practices.

First Data Loosened Oversight of FPS by Tripling Its Concurrence Level, Even As FPS Continued to Board Deceptive Merchants

109. Under the Processing Agreement, FPS was permitted to independently board and process high-risk merchants with annual transaction volumes of $1 million or less without obtaining prior approval or "concurrence" from First Data and Wells Fargo.

110. In July 2013, despite mounting problems with FPS's underwriting and boarding fraudulent merchants, First Data tripled FPS's concurrence level, permitting FPS to independently approve and open with no prior approval "any high-risk merchant" which First Pay anticipated would have less than $3 million in annual Visa and Mastercard volume.

111. First Data allowed FPS to maintain a $3 million concurrence level for the remainder of the processing relationship, until Wells Fargo terminated FPS in November 2014.

Even After Wells Fargo and First Data Named FPS an Excessive Risk ISO For the Second Time, First Data Still Tried to Grow FPS's High-Risk Business

112. In December 2013, Wells Fargo notified First Data that several FPS merchants had been placed in Visa's chargeback monitoring program in October 2013 and December 2013 for boarding unqualified nutraceutical accounts. At or around the same time, Wells Fargo designated FPS as an Excessive Risk ISO for the second time since August 2012.

113. In December 2013, in response to the designation, First Data created a report on FPS that identified five "unqualified or prohibited" accounts that were selling nutraceuticals and debt relief services, including merchants for the E.M. Systems Scheme, noting that "a merchant is selling a package for debt reduction – offering to lower interest on credit cards." First Data

emailed FPS about its failure to adequately underwrite the accounts, noting that FPS had failed to review the merchant applicants' websites and failed to detect that one of the merchants "had done this before" and was "an internal match due to chargeback issues."

114. In January 2014, Wells Fargo and First Data met to discuss the recent boarding of unqualified accounts. Days after the meeting, a First Data senior risk director sent a status report on FPS to First Data's vice-president of payment card compliance and others at First Data and Well Fargo:

> "First Pay has been coroneted Excessive Risk ISO for the second time around… It appears the ISO still has gaps within their risk monitoring and underwriting processes…
>
> While a profitable organization, the ISO is falling short on the required standards to effectively manage their portfolio below excessive risk status…

115. Despite these concerns, just two weeks later, First Data identified FPS as an "**ISO with Opportunities"** (emphasis in original) in a sales presentation that directed sales representatives to increase boarding of merchants in "undersold markets." The presentation was part of a 2014 First Data sales initiative to further penetrate high risk markets such as nutraceuticals, "investment programs," "fortune tellers," "mail order brides," "massage parlors," online gambling, outbound telemarketers, and "pyramid" multi-level marketers. First Data's senior credit officer emailed First Data's vice-president of risk management about the presentation, asking, "Are the suggested ISOs OK, meaning are they clean?"

116. Despite these reservations, in March 2014, First Data awarded Ko and FPS membership in its President's Club, the highest sales distinction reserved for First Data's top producing clients.

117. In June 2014, First Data's director for alternative markets emailed Ko directly

about the potential for FPS to grow business in undersold markets, noting that they were an "excellent revenue outlet source."

First Data Continued Processing for FPS's Fraudulent Merchants
Until It was Forced to Stop by Wells Fargo and Visa

118. In May 2014, Wells Fargo, First Data and FPS participated in a conference call to discuss FPS's continued high chargebacks and boarding of fraudulent merchant accounts. After the call, First Data's director of credit risk management emailed First Data's vice-president of compliance, as well as Wells Fargo's senior vice-president of acquiring sponsorship and vice-president of risk management, stating that the call "revealed that the ISO [FPS] has critical gaps within their underwriting and risk management processes." Around the same time, Wells Fargo met with First Data about its failure to connect and monitor FPS's fraudulent merchant accounts. A Wells Fargo Power Point presentation from the meeting, sub-titled "First Data's responsibility to keep ISOs clean," noted:

> "FD [First Data] appears to be concerned about ISOs' financials, not merchants' activities and associated risks; The focus appears to be on loss risk not reputational and or regulatory (FTC); FD is not making connection to seemingly related accounts. The risks are substantial."

119. In June 2014, First Data conducted an on-site audit of FPS for the first time since entering the Processing Agreement in 2010, despite Wells Fargo and First Data's own requirement that their ISOs receive an annual site visitation. First Data concluded in its audit report that

> "[FPS] failed to identify fraudulent businesses…and **does not have the appropriate processes, risk expertise, tools and/or independent oversight to effectively assess, monitor and manage risk associated with high risk e-commerce**." (emphasis in original).

120. After reaching this conclusion, First Data continued to process over $50 million

through FPS's high-risk e-commerce accounts with an average chargeback ratio of 22.7% over the next five months, including millions of charges for the E.M. Systems and Beckish Schemes.

121. In July 2014, a First Data risk management director emailed First Data's regional business director and vice-president of risk management about FPS: "I am aware this ISO has had issues in the past with excessive chargebacks and unqualified accounts."

122. In August 2014, Wells Fargo contacted First Data's vice-president of risk management about 269 FPS "suspect bad merchants" that had been identified in a request for information from Visa, including merchant accounts for the Thrive Learning, E.M. Systems, and Beckish Schemes. Wells Fargo noted that they "that appear to have been opened solely to funnel fraudulent transactions."

123. In September 2014, Visa's head of global brand protection contacted Wells Fargo and First Data regarding scores of FPS merchant accounts it believed were running a fraudulent billing scheme based on a review of online consumer complaint boards. In response, Wells Fargo provided Visa with processing statistics for the suspected merchants, noting that the accounts identified had an aggregate chargeback ratio of approximately 32% in August 2014. A Wells Fargo report sent to First Data's risk management director noted:

> "Visa is currently investigating numerous accounts recently boarded, 16 accounts are being investigated due to excessive disputes from card issuing bank, 55 accounts which processed over 12,000 chargebacks are being considered for VISA HRMCP program and approximately 200 accounts were identified for fraudulent activities. Overall, processing statistics is trending negatively; chargebacks have increased 10 times over within the last 6 months."

In fact, these were merchant accounts for the Beckish Scheme.

124. Around the same time, Wells Fargo's senior vice-president of acquiring sponsorship forwarded an email from Visa to a First Data vice president of security and risk

management: "What steps did First Data take to validate the true validity of the principals?" First Data's regional business directors and risk management directors also emailed Ko directly about the Visa inquiry.

125. In September 2014, Wells Fargo notified FPS and First Data that it would terminate the Processing Agreement in November 2014. In response to the planned termination by Wells Fargo, First Data and FPS sought a new acquiring bank to sponsor FPS's processing activity. First Data's vice-president of ISO sales emailed internally that "Vincent texted me on Friday that he has a clearing bank, wants an FSP [full service processing] agreement and a DB [Deutsche Bank] wholesale start-up." First Data's senior vice-president of ISO client sales replied, "Good."

126. In October 2014, Wells Fargo's executive vice-president emailed First Data's corporate parent, First Data Corporation's ("FDC"), general counsel, asking,

> "Why is First Data signing ISOs like [First Pay]? They are going to get First Data and Wells Fargo in trouble with the FTC and CFPB due to consumer deceptive practices…we cannot continue to sponsor First Data's ISO business if there is no oversight, processes and good policies in place."

127. The same month, Wells Fargo noted in a PowerPoint presentation that First Data:

> "Failed to identify fraudulent accounts during the file review segment of their visit at First Pay;
> Missed the use of non-compliant descriptors;
> Slow to react to a severe increase in cb [chargeback] numbers;
> Failed to identify an influx of very unusual, new accounts being boarded…
> FD [First Data] does not perform physical reviews neither (sic) at underwriting or annually."

128. In October 2014, First Data sent a letter to Ko advising that FPS had 200,000 chargebacks in 2014 and that First Data was increasing FPS's reserve account to $10 million. Around the same time, First Data proposed to Wells Fargo to extend the termination date of the

Processing Agreement in order to acquire and process for FPS's retail merchant accounts, *i.e.* accounts other than high-risk accounts. First Data's vice-president of security and risk management emailed First Data's chief credit officer about the proposed extension:

> "Do we really want to do this?... [W]e are not sure that we agree that this ISO was being duped by a sales agent and had poor risk management processes…
>
> First Pay has been on the problem ISO list since 2012…[First Data Risk Management] uncovered multiple accounts in 2012 where they have been asked to close accounts for Continuity/Negative Renewal, Chargebacks, ecommerce, etc…
>
> It seems like they have been in this business for awhile…."

129. First Data did not stop processing for FPS's high-risk merchants until October 2014, when termination of the Processing Agreement was imminent. "This was accomplished by shutting off [Ko's] system access," a First Data risk director told Wells Fargo.

130. The Processing Agreement terminated in November 2014. After the termination, First Data's vice-president of risk management identified almost 100 FPS merchants boarded in 2014 that had "NO sign of a product/service."

First Data and FPS's Conduct Triggered Remedial Action by Visa

Visa Required First Data to Pay $18.7 Million in Restitution and Banned the Company from Boarding ISOs or High-risk Merchants

131. In November 2014, Visa's head of global brand protection wrote to Wells Fargo about imminent fines related to a group of merchants for the Beckish Scheme that "were introduced into the payment systems by your agents First Data and FPS." Visa's letter stated that the incident "was caused by Wells Fargo Bank and First Data's failure to provide adequate oversight and control of its agent portfolio." The letter sought from Wells Fargo an explanation of "why First Data permitted the group of 62 merchants to be boarded by First Pay after this

agent was identified as High Risk by Wells Fargo…"

132. In December 2014, Visa wrote to First Data and Wells Fargo having determined the merchants "caused undue harm to the goodwill of the Visa Payment System by generating 133,354 chargebacks at a 34% chargeback rate and a 40% fraud to sales ratio." In the same month, Visa banned Wells Fargo and First Data from contracting with new ISOs and from processing charges for new high-risk merchants through its network until the entire First Data/Wells Fargo merchant portfolio could be audited by a third party accounting firm.

133. In April 2015, an audit conducted by Pricewaterhouse Coopers found significant failures in First Data's risk management practices, including "no controls" over high-risk merchant boarding, deficient merchant transaction monitoring, and failures in due diligence of its agents. Since that time, First Data has resumed processing charges for new high-risk merchants through Visa.

After FPS Was Terminated for Boarding Fraudulent Merchant Accounts, First Data Acquired FPS's Portfolio and Hired its President

134. In or around December 2014, First Data acquired FPS's merchant accounts and hired most of FPS's employees.

135. In September 2015, First Data asked Wells Fargo to allow former FPS employees employed at First Data to resume soliciting high-risk merchants. Wells Fargo granted the request on the condition that the former FPS employees were not "associated with or related to Vincent Ko" and that First Data could confirm that "Vincent Ko has no influence."

136. In January 2017, First Data hired Ko as a vice-president of strategic partnerships. Since then, Ko hired at least 15 sales agents to solicit prospective merchants.

137. Based on the facts and violations of law alleged in this Complaint, the FTC has

reason to believe that Defendants are violating or are about to violate laws enforced by the Commission because, among other things:

a. Defendants engaged in their unlawful acts and practices repeatedly over a period of almost 3 years;

b. Ko continued his unlawful acts or practices despite knowledge and direct evidence that his company was boarding merchants which were shell companies or other companies engaged in fraud;

c. First Data continued its unlawful acts and practices despite knowledge that it was processing transactions for, and allowing FPS to board, shell companies or other companies engaged in fraud;

d. First Data continued its unlawful acts and practices despite knowledge of exorbitant chargeback rates and chargeback narratives that described consumer deception; and

e. First Data continued its unlawful acts and practices despite knowledge of numerous government and industry inquiries into FPS and its merchants' fraudulent conduct.

VIOLATIONS OF THE FTC ACT

138. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce." Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I
UNFAIR PAYMENT PROCESSING PRACTICES
(as to all Defendants)

139. In numerous instances, Defendants have:

a. Opened or maintained payment processing accounts for merchants that were shell companies or other companies engaged in fraud;

b. Processed transactions to consumers' accounts for merchants that were shell companies or engaged in fraud;

c. Failed to timely terminate merchants that were shell companies or other companies engaged in fraud; and

d. Ignored evidence of fraudulent activity on merchant accounts.

140. Defendants' actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

141. Therefore, Defendants' acts or practices, as set forth in Paragraph 139, constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a) and (n).

VIOLATIONS OF THE TSR

142. In 1994, Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101–6108. The FTC adopted the original TSR in 1995, extensively amended it in 2003, and amended certain provisions thereafter. 16 C.F.R. Part 310.

143. Under the TSR, a "merchant" means a person who is authorized under a written contract with an acquirer to honor or accept credit cards, or to transmit or process for payment credit card payments, for the purchase of goods or services or a charitable contribution. 16

C.F.R. § 310.2(u).

144. It is a violation of the TSR for any person to employ, solicit, or otherwise cause a merchant, or an employee, representative, or agent of the merchant, to present to or deposit into the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchant; 16 C.F.R. § 310.3(c)(2).

145. The TSR also prohibits a person from providing substantial assistance or support to any seller or telemarketer when that person "knows or consciously avoids knowing" that the seller or telemarketer is engaged in any act or practice that violates Section 310.3(c). 16 C.F.R. § 310.3(b).

146. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c) and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT II
CREDIT CARD LAUNDERING
(as to Defendant Ko)

147. In numerous instances and without the express permission of the applicable credit card system, Defendant Ko has employed, solicited, or otherwise caused shell companies, or representatives or agents of those shell companies, to present to or deposit into, the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the shell companies, as described in Paragraphs 20–137.

148. Defendant Ko's acts or practices, as described in Paragraph 147, are deceptive

telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(c)(2).

COUNT III
ASSISTING AND FACILITATING CREDIT CARD LAUNDERING
(as to Defendant First Data)

149. In numerous instances and without the express permission of the applicable credit card system, Defendant First Data has provided substantial assistance or support to persons whom Defendant First Data knew, or consciously avoided knowing, employed, solicited, or otherwise caused shell companies, or representatives or agents of those shell companies, to present to or deposit into, the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the shell companies, as described in Paragraphs 20–137, in violation of Section 310.3(c)(2) of the TSR, 16 C.F.R. § 310.3(c)(2).

150. Defendant First Data's acts or practices, as described in Paragraph 149, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(b).

COUNT IV
ASSISTING AND FACILITATING DECEPTIVE REPRESENTATIONS
(as to all Defendants)

151. In numerous instances, the Defendants, or their agents or subagents, have provided substantial assistance or support to sellers or telemarketers whom the Defendants or their agents or subagents knew, or consciously avoided knowing:

a. Induced consumers to pay for goods and services through the use of false or misleading statements, including but not limited to, false or misleading statements in connection with the telemarketing of debt relief services, in violation of Section 310.3(a)(2)(x) of the TSR, 16 C.F.R. § 310.3(a)(2)(x);

b. Charged an advance fee for debt relief services, in violation of Section 310.3(a)(5)(i) of the TSR, 16 C.F.R. § 310.3(a)(5)(i); or

c. Induced consumers to pay for goods and services through the use of false or misleading statements in connection with any material aspect of an investment opportunity, including, but not limited to risk, liquidity, earnings potential, or profitability, in violation of Section 310.3(a)(2)(vi) of the TSR, 16 C.F.R. § 310.3(a)(2)(vi).

152. The Defendants' acts or practices, as set forth in Paragraph 151, constitute deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(b).

CONSUMER INJURY

153. Consumers throughout the United States are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act and TSR. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THE COURT'S POWER TO GRANT RELIEF

154. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

155. Section 19 of the FTC Act, 15 U.S.C. § 57b, and Section 6(b) of the

Telemarketing Act, 15 U.S.C. § 6105(b), authorize this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the TSR, including the rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies.

PRAYER FOR RELIEF

156. Wherefore, Plaintiff, pursuant to Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b) and 57b, Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b), and the Court's own equitable powers, requests that the Court:

a. Enter a permanent injunction to prevent future violations of the FTC Act and TSR by Defendants;

b. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, and TSR, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

c. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

ALDEN F. ABBOTT,
General Counsel

Dated: May 19, 2020

NICHOLAS M. MAY*
ANNA M. BURNS*
MICHAEL A. BOUTROS*
Federal Trade Commission
Southeast Region
225 Peachtree Street NE, Suite 1500
Atlanta, GA 30303
(404) 656-1360; nmay@ftc.gov
(404) 656-1350; aburns@ftc.gov
(404) 656-1351; mboutros@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

*Application for admission *pro hac vice* forthcoming